BayRS Version 14.20

Part No. 308647-14.20 Rev 00
September 2000

600 Technology Park Drive
Billerica, MA 01821-4130

Configuring VRRP Services

Copyright © 2000 Nortel Networks

All rights reserved. September 2000.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

NORTEL NETWORKS is a trademark of Nortel Networks.

BCN and BLN are registered trademarks and ANH, ASN, BayRS, BCC, and System 5000 are trademarks of Nortel Networks.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks NA Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as “Software” in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept

these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License grant. Nortel Networks NA Inc. (“Nortel Networks”) grants the end user of the Software (“Licensee”) a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks’ and its licensors’ confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee’s facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee’s intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee’s requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor’s product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT

SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks, 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Before You Begin xi
Text Conventions xii
Acronyms xiii
Hard-Copy Technical Manuals xiv
How to Get Help xiv

Chapter 1
VRRP Concepts

About VRRP 1-1
Master Virtual Router 1-2
Backup Virtual Routers 1-2
Critical IP Interfaces 1-2
VRRP Messaging 1-2
Planning Your Network 1-3
Sample Configurations 1-3

Chapter 2
Starting VRRP Services

Starting Configuration Tools 2-1
Configuring a Virtual Router 2-2
Configuring VRRP on a Multinetted Interface 2-2
Configuring VRRP Over IP 2-3
Using the BCC 2-3
Configuring a Physical Interface 2-3
Configuring an IP Interface 2-4
Configuring a Virtual Router 2-4
Using Site Manager 2-5

Configuring VRRP in an MPOA Network 2-7
Using the BCC 2-7
Adding ATM to the Configuration 2-8
Enabling Signaling 2-8
Defining a LAN Emulation Client Service Record 2-9
Creating an MPOA Service Record 2-9
Adding an MPOA Server (MPS) 2-10
Adding IP, RIP or OSPF, and NHRP to the LEC Service Record 2-10
Mapping an MPS to a LEC 2-11
Adding VRRP to the LEC Service Record 2-11
Using Site Manager 2-12
Creating an ATM Circuit 2-13
Adding a LANE Service Record 2-14
Creating an MPOA Service Record 2-15
Adding an MPOA Server (MPS) 2-16
Adding IP, RIP or OSPF, and NHRP to the LEC Service Record 2-17
Mapping an MPS to the LEC Service Record 2-19
Adding VRRP to the LEC Service Record 2-20

Chapter 3
Customizing VRRP

Disabling and Reenabling a Virtual Router 3-2
Changing the IP Address Backed Up by a Virtual Router 3-3
Setting the Priority of the Virtual Router 3-4
Setting the Advertisement Interval 3-6
Setting the Critical IP Interface Address 3-8
Enabling or Disabling IPX Backup 3-9
Enabling or Disabling IGMP Backup 3-11
Setting the Token Ring Address 3-13

Appendix A
Site Manager Parameters

Add Virtual Router Parameters A-2
VRRP Configuration Parameters A-4

Appendix B
Monitoring VRRP Using the BCC show Commands

Online Help for show Commands B-1
show vrrp critical-ip-addresses B-2
show vrrp mac-addresses B-2
show vrrp summary B-3

Glossary

Index

Figures

Figure 1-1. Using VRRP with One Master and One Backup Virtual Router 1-3
Figure 1-2. Using VRRP and Performing Load-Balancing 1-4
Figure 1-3. Using VRRP with a Critical IP Interface 1-5
Figure 1-4. Sample Invalid Virtual Router Configuration 1-6
Figure A-1. Add Virtual Router Window A-2
Figure A-2. IP VRRP Configuration Parameters Window A-4

Preface

This guide describes the Virtual Router Redundancy Protocol (VRRP) and what you do to start and customize VRRP services on a Nortel Networks™ router.

You can use the Bay Command Console (BCC™) or Site Manager to configure VRRP services on a router. In this guide, you will find instructions for using both the BCC and Site Manager.

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (see the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Nortel Networks BayRS™ and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is: **ping** <*ip_address*>, you enter: **ping 192.32.10.12**
bold text	Indicates command names and options and text that you need to enter. Example: Enter **show ip** {**alerts** | **routes**}. Example: Use the **dinfo** command.
braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you must enter either: **show ip alerts** or **show ip routes**, but not both.
italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is: **show at** <*valid_route*> *valid_route* is one variable and you substitute one value for it.
`screen text`	Indicates system output, for example, prompts and system messages. Example: `Set Trap Monitor Filters`

separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you enter either: **show ip alerts** or **show ip routes**, but not both.

Acronyms

This guide uses the following acronyms:

ATM	asynchronous transfer mode
ARP	Address Resolution Protocol
BUS	broadcast and unknown server
ELAN	emulated local area network
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPX	Internetwork Packet Exchange
LAN	local area network
LANE	LAN emulation
LEC	LAN emulation client
MAC	media access control
MIB	management information base
MPC	MPOA client
MPOA	Multi-Protocol Over ATM
MPS	MPOA server
VRID	virtual router identifier
VRRP	Virtual Router Redundancy Protocol

Hard-Copy Technical Manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the support.baynetworks.com/library/tpubs/ URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe Acrobat Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at www.adobe.com to download a free copy of Acrobat Reader.

You can purchase selected documentation sets, CDs, and technical publications through the Internet at the www1.fatbrain.com/documentation/nortel/ URL.

How to Get Help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
EMEA	(33) (4) 92-966-968
North America	(800) 2LANWAN or (800) 252-6926
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the www12.nortelnetworks.com/ URL and click ERC at the bottom of the page.

Chapter 1
VRRP Concepts

This chapter describes VRRP concepts you need to know before you begin configuring a VRRP router.

Topic	Page
About VRRP	1-1
Master Virtual Router	1-2
Backup Virtual Routers	1-2
Critical IP Interfaces	1-2
VRRP Messaging	1-2
Planning Your Network	1-3

About VRRP

The Virtual Router Redundancy Protocol (VRRP), which runs over IP, enables you to configure router redundancy. This redundancy protects a network from the irrecoverable failure of one or more IP interfaces and eliminates any single point of failure within your network. In addition to configuring VRRP over IP, you can also configure VRRP on an ATM network that is configured with Multi-Protocol over ATM (MPOA).

VRRP manages a virtual router, which is a software-defined object that corresponds to an IP address on a LAN segment. A virtual router typically exists on multiple routers running VRRP (known as VRRP routers). One of the VRRP routers acts as the master virtual router for an IP address, while other VRRP routers act as backup virtual routers.

You identify each virtual router using a virtual router identifier (VRID) and a virtual router IP address. All VRRP routers on a LAN segment must have the same VRID and virtual router IP address. You can, however, use a VRID on more than one LAN as long as you pair it with a different virtual router IP address. Each virtual router is restricted to a single LAN.

Master Virtual Router

The master virtual router is responsible for forwarding the traffic destined for the MAC address associated with the virtual router IP address. A VRRP router with the highest priority assumes the responsibilities of the master virtual router. When the master virtual router fails, one of the backup virtual routers becomes the master virtual router.

Backup Virtual Routers

If the master virtual router becomes unavailable or if it is not functioning normally, VRRP dynamically switches over to one of the backup virtual routers, in the order of the priority you set.

If more than one backup virtual router has the same priority, the VRRP router with the greater primary IP address becomes the new master virtual router.

Critical IP Interfaces

You can establish a critical IP address, which is a physical IP interface on a local router that is not running VRRP. If that critical IP interface fails, then VRRP switches to another VRRP router. Refer to Figure 1-3 on page 1-5 for a sample VRRP configuration using a critical IP interface.

VRRP Messaging

VRRP generates VRRP advertisement messages as IP multicast datagrams, enabling VRRP to operate over a variety of multiaccess LAN technologies that support IP multicasting. Only the master virtual router transmits VRRP advertisements.

Planning Your Network

You can use VRRP to target stub networks with hosts having default gateway addresses to provide redundancy for IP addresses. To avoid a single point of failure, you should configure the default gateway IP address as the virtual router IP address on multiple IP interfaces on different physical routers. Refer to the following sample configurations when determining how to configure VRRP in your network.

Sample Configurations

The configuration in Figure 1-1 shows a simple VRRP scenario in which both router A and router B are running VRRP. The end hosts install a default route to the IP address of router A, which serves as the master virtual router for virtual router 1. If router A fails, then router B becomes the master virtual router for virtual router 1.

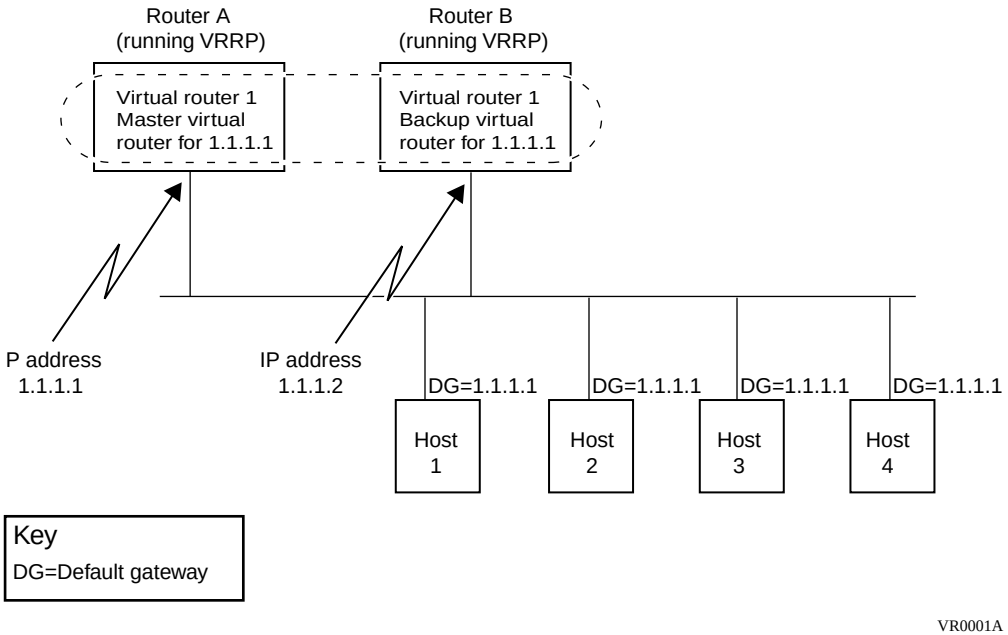

Figure 1-1. Using VRRP with One Master and One Backup Virtual Router

The configuration in Figure 1-2 shows that half of the hosts install a default route to VRRP router A's IP address (1.1.1.1), and the other half install a default route to VRRP router B's IP address (1.1.1.2). Using two different default routes balances the load for outgoing traffic, and also provides full redundancy.

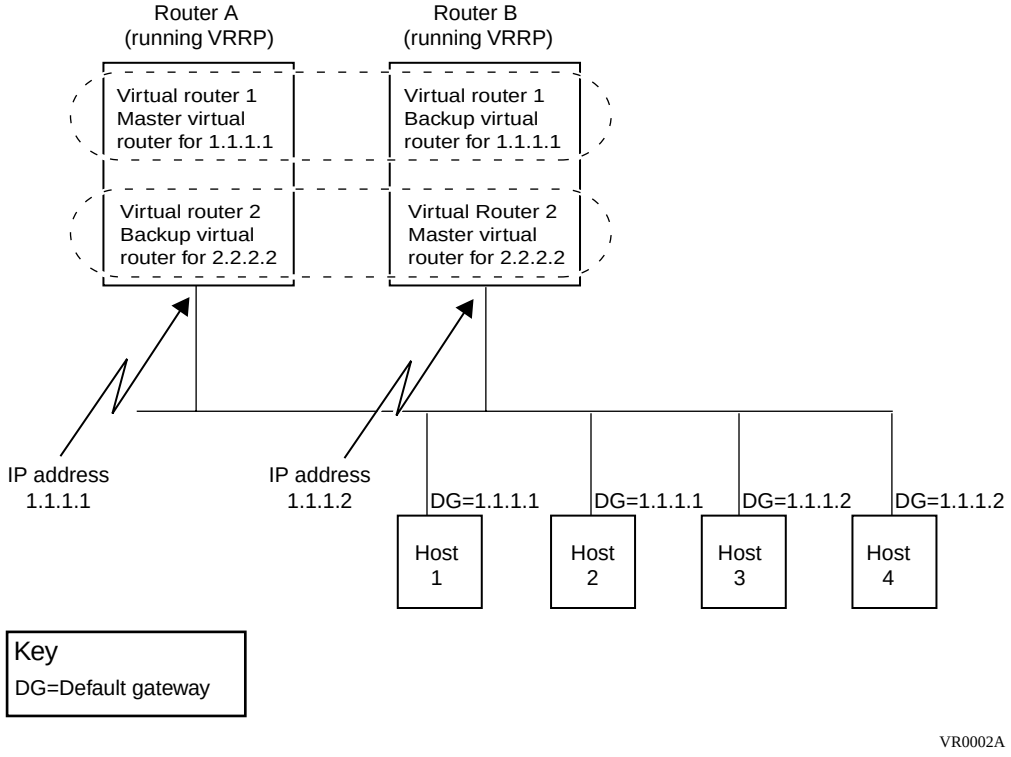

Figure 1-2. Using VRRP and Performing Load-Balancing

The configuration in Figure 1-3 shows that IP address 1.1.1.1 connects to external networks. If that connection fails and the virtual router 1 on router B continues to forward traffic, you still lose connectivity to external networks. However, if you designate IP address 1.1.1.1 as the critical IP address for virtual router 1 on router B, and IP address 1.1.1.1 fails, then virtual router 1 on router A becomes the master virtual router and begins forwarding traffic.

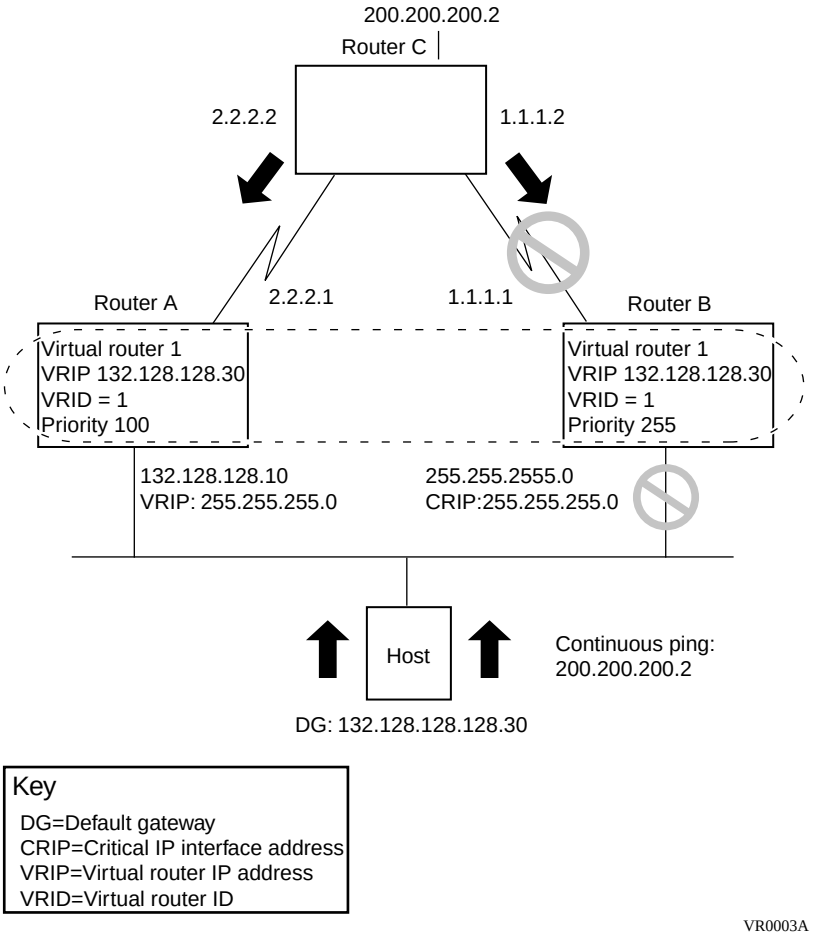

Figure 1-3. Using VRRP with a Critical IP Interface

Figure 1-4 shows an invalid VRRP configuration; that is, the virtual router with primary IP address 1.1.1.1 is not configured on a VRRP router that has a physical interface with IP address 1.1.1.1. You must always configure a virtual router whose IP address physically exists on the LAN. For example, you must configure virtual router 1 on router A, because the IP address of virtual router 1 is the same as the physical address of router A.

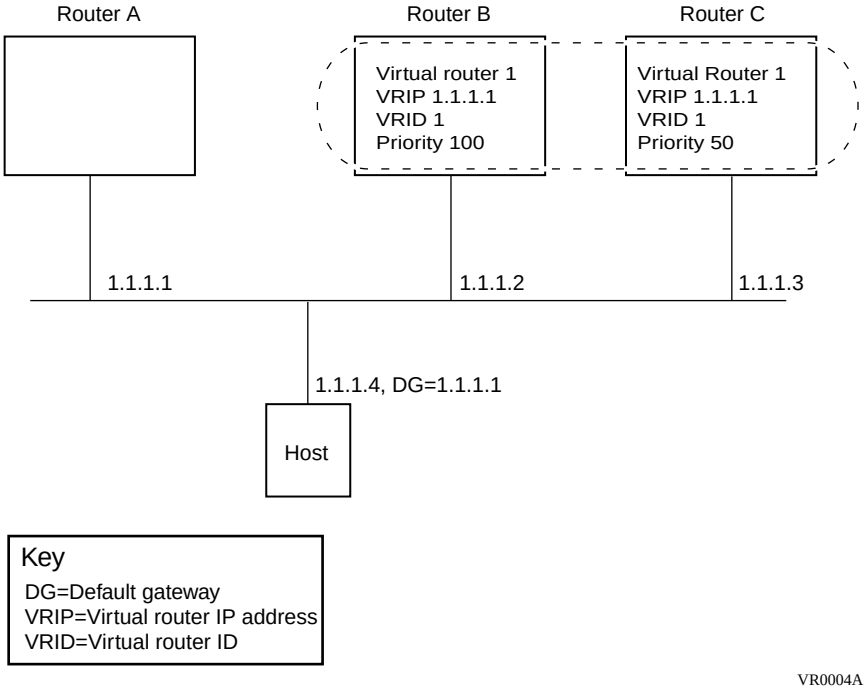

Figure 1-4. Sample Invalid Virtual Router Configuration

Chapter 2
Starting VRRP Services

You must configure IP services on a router before you can configure VRRP. This chapter explains how to configure a router running over IP, and how to configure a router on an ATM network running MPOA.

- For information about how to configure IP, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*.
- For information about how to configure ATM, see *Configuring ATM Services*.
- For information about how to configure MPOA, see *Configuring MPOA and NHRP Services*.

You can create a basic virtual router configuration by supplying only the required configuration information and accepting the default values for all other parameters.

Starting Configuration Tools

Before configuring VRRP, refer to the following user guides for instructions on how to start and use the Nortel Networks configuration tool of your choice.

Configuration Tool	User Guide
Bay Command Console (BCC)	*Using the Bay Command Console (BCC)*
Site Manager	*Configuring and Managing Routers with Site Manager*

These guides also describe generically how to create and modify a device configuration.

Configuring a Virtual Router

When configuring a virtual router, you must supply the following:

- Primary IP address

  The primary IP address associates a virtual router with the IP address of the physical interface. You cannot change the primary IP address after you configure a virtual router. If this primary IP address matches the virtual router IP address, the virtual router will have the highest priority (255) and become the master virtual router.

Caution: You should not configure an Ethernet interface as the master virtual router on an ANH™ router. The Ethernet interface does not go down if you remove the Ethernet cable. As a result, it remains in the master state.

- Virtual router ID

  The virtual router ID (VRID) identifies the virtual router. VRRP uses the virtual router ID to calculate the virtual router's virtual MAC address. If the virtual router is in the primary virtual router state, it responds to all Address Resolution Protocol (ARP) requests using the IP address of the virtual router with its virtual MAC address, not its physical MAC address. You cannot change the virtual router ID after you configure a virtual router.

- Virtual router IP address

  The virtual router IP address identifies the IP address that the virtual router will use.

You can configure as many as 50 virtual routers. To configure a router running over IP, see "Configuring VRRP Over IP" on page 2-3. To configure a router on an ATM network, see "Configuring VRRP in an MPOA Network" on page 2-7.

Configuring VRRP on a Multinetted Interface

To configure VRRP on a multinetted interface, you must:

- Configure a virtual router for each IP address on the multinetted interface that you want to back up.
- Use the same VRID for all the virtual routers.

For example, to back up two different IP addresses that are multinetted on one interface, configure a virtual router for each IP address. Use a different IP address for each virtual router, but use the same VRID for both.

Configuring VRRP Over IP

You can use the BCC or Site Manager to start IP on the router and configure VRRP.

Using the BCC

Complete the following tasks to start IP and configure VRRP on the router:

1. Configure a physical interface on an available slot/connector.
2. Configure an IP interface on the physical interface.
3. Configure a virtual router.

Configuring a Physical Interface

To configure a physical interface on a slot and connector, navigate to the top-level box prompt (box or stack) and enter:

<*interface_type*> **slot** <*slot_number*> **[module** <*module_number*>**] connector** <*connector_number*>

interface_type is the name of a link module on the router.

slot_number is the number of the slot on which the link or net module is located.

module_number is the net module number (ASN™ and System 5000™ routers only).

connector_number is the number of a connector on the link or net module.

For example, the following command configures an Ethernet interface on slot 2, connector 2:

```
box# ethernet slot 2 connector 2
ethernet/2/2#
```

Configuring an IP Interface

To configure an IP interface on a physical interface, navigate to the prompt for the physical interface and enter:

ip address <*address*> **mask** <*mask*>

address and *mask* are a valid IP address and its associated mask, expressed in dotted-decimal notation.

For example, the following command configures IP interface 2.2.2.2/255.0.0.0 on an Ethernet physical interface on slot 2, connector 2:

```
ethernet/2/2# ip address 2.2.2.2 mask 255.0.0.0
ip/2.2.2.2/255.0.0.0#
```

An IP interface is now configured on the Ethernet interface with default values for all interface parameters. When you configure an IP interface, the BCC also configures IP globally on the router with default values for all IP global parameters.

To customize your IP interface by modifying the IP global and interface parameters, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*.

Configuring a Virtual Router

To configure a virtual router begin at the top-level box prompt and enter:

ip

The IP global prompt appears. Note that you can configure a virtual router on an IP interface that does not exist.

At the IP global prompt, enter the following:

vrrp primary-ip-address <*primary_ip_address***> vr-id <***vr_id***> vr-ip-address <***vr_ip_address***>**

primary_ip_address is the IP address of the physical interface with which the virtual router is associated.

vr_id is the virtual router identifier configured in the range of 1 to 255.

vr_ip_address is the IP address that the virtual router uses.

The primary IP address and the virtual router IP address must form a unique pair and must also be on the same subnet.

Note: You can also configure a virtual router using the shortened command format:

vrrp <*primary_ip_address*>/<*vr_id*> **vr-ip-address** <*vr_ip_address*>

For example, to configure a virtual router with a primary IP address of 192.41.31.21, a virtual router ID of 2, and a virtual router IP address of 192.41.31.22, enter the following:

```
box# ip
ip# vrrp primary-ip-address 192.41.31.21 vr-id 2 vr-ip-address 192.41.31.22
vrrp/192.41.31.21/2#
```

Using Site Manager

Before you can select a protocol to run on the router, you must first configure a circuit that the protocol can use as an interface to an attached network. For information and instructions, see *Configuring WAN Line Services* and *Configuring Ethernet, FDDI, and Token Ring Services*.

When you have successfully configured the circuit, the Select Protocols window opens. To start IP, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Select Protocols window, select **IP**. Then click on **OK**.	The IP Configuration window opens.
2. Set the following parameters: • **IP Address** • **Subnet Mask** • **Transmit Bcast Addr** • **UnNumbered Assoc Addr** Click on **Help** or see the parameter descriptions in *Configuring IP, ARP, RARP, RIP, and OSPF Services.*	
3. Click on **OK**.	You return to the Configuration Manager window.

An IP interface is now configured with default values for all interface parameters. When you configure an IP interface, Site Manager also configures IP globally on the router with default values for all IP global parameters.

To customize your IP interface by modifying the IP global and interface parameters, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*.

Caution: If you are configuring virtual routers on the IP interface used as the Site Manager management console, do not add or modify a backup virtual router before you create a master virtual router. Otherwise, you can lose connectivity to the router when dynamically configuring virtual routers. To prevent this, use local or remote mode when configuring a virtual router.

To configure a virtual router using Site Manager, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on **Add**.	The Add Virtual Router window opens.
5. Set the following parameters: • **Primary IP Address** • **Virtual Router ID** • **Virtual Router IP Address** Click on **Help** or see the parameter descriptions starting on page A-3.	
6. Click on **OK**.	You return to the IP VRRP Configuration Parameters window.

Configuring VRRP in an MPOA Network

Before you can configure VRRP in an MPOA network, you have to start ATM on the router, define a switched virtual circuit (SVC) service record, and select LAN emulation (LANE) as the data encapsulation type.

SVCs use signaling messages to dynamically establish, maintain, and clear a switched virtual connection at the UNI. These messages (as defined by the Q.2931 standard for signaling protocols) allow the router to assess the availability of an ATM end point (device), establish a connection with that device, maintain that connection for the duration of data transfer, and then clear the connection when the transfer is complete.

LANE extends the ATM network to LANs. Selecting LANE to run on an SVC service record defines that service record as belonging to an emulated LAN (ELAN). Any protocols on that service record operate as if they were running over a traditional Ethernet or token ring LAN.

MPOA operates at layer 3 and enables IP to run over ATM networks. MPOA maps routed and bridged traffic flows to ATM SVCs. Since this technique maps traffic to virtual channels, it removes many performance limitations. Instead of individual packets making multiple hops, MPOA creates network "shortcuts" between source and destination clients. This is generally referred to as *cut-through* or *zero-hop routing*.

Using the BCC

Complete the following tasks to start ATM, and then configure MPOA and VRRP on a router:

1. Add ATM to the configuration.
2. Enable ATM signaling.
3. Define a LAN emulation client (LEC) service record.
4. Create an MPOA service record.
5. Add an MPOA Server (MPS).
6. Add IP, RIP or OSPF, and NHRP to the LEC service record.
7. Map an MPS to a LEC.
8. Add VRRP to the LEC service record.

Adding ATM to the Configuration

To add ATM to the configuration, navigate to the top-level prompt and enter:

atm slot <*slot_number*> **[pci-slot** <*slot_number*>**][module** <*module_number*>**] connector** <*connector_number*>

slot_number is the number of the chassis slot containing the link module.

pci_slot is the pci-slot number of the ATM-E1/ATM-T1 line.

module_number is a convention used for other routers within the System 5000 chassis. You need only enter a module number when configuring an ATM interface in the System 5000 chassis (that is, the Model 5782 Centillion Multiprotocol Engine). The module number for the ATM interface is always 2.

connector_number is the number of a connector on the link module.

Note: The top-level prompt for BCC configuration on the System 5000 platform is "stack." However, the remainder of this guide uses the "box" prompt associated with the BN platform in its examples.

For example, the following commands add ATM to a configuration.

To add ATM to the BN configuration on slot 5, connector 1:

```
box# atm slot 5 connector 1
atm/5/1#
```

Enabling Signaling

To enable signaling on an ATM interface, navigate to the ATM prompt and enter:

signaling

For example, the following command enables UNI V3.0 (default) signaling on slot 5, connector 1:

```
atm/5/1# signaling
signaling/5/1#
```

Defining a LAN Emulation Client Service Record

To define a LAN emulation client (LEC) service record, navigate to the ATM interface prompt and enter:

lec-service <*service_name*>

service_name is a unique text string that you assign to the service record.

For example, the following command defines a LEC service record with the name "newyork" on ATM slot 5, connector 1:

```
atm/5/1# lec-service newyork
lec-service/newyork#
```

Creating an MPOA Service Record

To create an MPOA service record, navigate to the appropriate ATM interface prompt and enter:

mpoa-service

For example, on a System 5000 router, the following command sequence:

- Creates an ATM interface on slot 5, module 3, connector 1.
- Creates an MPOA service on the ATM interface.

```
stack# atm slot 5 module 3 connector 1
atm/5/3/1# signaling
signaling/5/3/1# back
atm/5/3/1# mpoa-service
mpoa-service/5/3/1#
```

On a BLN®/BCN® router, the commands are identical, except that you do not specify a module number for the ATM interface:

```
box# atm slot 5 connector 1
atm/5/1# signaling
signaling/5/1# back
atm/5/1# mpoa-service
mpoa-service/5/1#
```

Adding an MPOA Server (MPS)

To add an MPS, navigate to the desired MPOA service prompt and enter:

mps mps-name <*mps-name*>

For example, on a System 5000 router, the following command adds an MPS named “eastcoast” to an MPOA service:

```
mpoa-service/5/3/1# mps mps-name eastcoast
mps/eastcoast#
```

Adding IP, RIP or OSPF, and NHRP to the LEC Service Record

To add IP, RIP or OSPF, and NHRP to an existing LEC service:

1. **Navigate to the appropriate lec-service prompt and enter:**

   nhrp

2. **Navigate back to the lec-service prompt, and enter:**

   ip address <*IP_address*> **mask** <*subnet_mask*>

3. **At the resulting IP interface prompt, add the desired routing protocol (RIP or OSPF):**

   rip

For example, on a System 5000 router, the following BCC commands navigate to the lec-service named “newyork” and add NHRP, IP, and RIP to that service:

```
stack# atm/5/3/1
atm/5/3/1# lec-service/newyork
lec-service/newyork# nhrp
nhrp/newyork# back
lec-service/newyork# ip address 1.2.3.4 mask 255.0.0.0
ip/1.2.3.4/255.0.0.0# rip
rip/1.2.3.4#
```

When you add NHRP to any ATM LEC service, the BCC automatically creates the global NHRP object at root level if you have not already done so.

Mapping an MPS to a LEC

To map an MPS to an LEC service, navigate to that LEC service and enter:

mpoa-server mps-name <*mps-name*>

For example, on a System 5000 router, the following BCC commands navigate to the LEC service “newyork” and map the MPS named “eastcoast” to it:

```
stack# atm/5/3/1
atm/5/3/1# lec-service/newyork
lec-service/newyork# mpoa-server mps-name eastcoast
mpoa-server/newyork#
```

Adding VRRP to the LEC Service Record

To configure a virtual router begin at the top-level box prompt and enter:

ip

The IP global prompt appears. Note that you can configure a virtual router on an IP interface that does not exist.

At the IP global prompt, enter the following:

vrrp primary-ip-address <*primary_ip_address***> vr-id <***vr_id***> vr-ip-address <***vr_ip_address***>**

primary_ip_address is the IP address of the physical interface with which the virtual router is associated.

vr_id is the virtual router identifier configured in the range of 1 to 255.

vr_ip_address is the IP address that the virtual router uses.

The primary IP address and the virtual router IP address must form a unique pair and must also be on the same subnet.

Note: You can also configure a virtual router using the shortened command format:
vrrp <*primary_ip_address*>/<*vr_id*> **vr-ip-address** <*vr_ip_address*>

For example, to configure a virtual router with a primary IP address of 192.41.31.21, a virtual router ID of 2, and a virtual router IP address of 192.41.31.22, enter the following:

```
box# ip
ip# vrrp primary-ip-address 192.41.31.21 vr-id 2 vr-ip-address 192.41.31.22
vrrp/192.41.31.21/2#
```

Using Site Manager

Complete the following tasks to start ATM, and then configure MPOA and VRRP on a router:

1. Create an ATM circuit.
2. Add a LANE service record.
3. Create an MPOA service record.
4. Add an MPOA Server (MPS).
5. Add IP, RIP or OSPF, and NHRP to the LEC service record.
6. Map an MPS to a LEC.
7. Add VRRP to the LEC service record.

Creating an ATM Circuit

To create an ATM circuit, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, for the Passport 5430 only, in slot 1, pci slot 1, module 2, click on the ATM T1/E1 link module (**ATM1**). For all other systems that support ATM, click on an ATM link module interface (**ATM1**).	The Add Circuit window opens.
2. Click on **OK** to accept the default circuit name.	The Select Connection Type window opens.
3. Click on **ATM**.	The Initial ATM Signaling Config window opens.
4. Click on **OK** to accept the default settings.	The Edit ATM Connector window opens.
5. Go to the next section to define a service record on the circuit.	

Note: Accepting the defaults in the Initial ATM Signaling Config window enables signaling on the interface.

Adding a LANE Service Record

To add a LANE service record, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on an ATM link module interface (**ATM1**).	The Select Connection Type window opens.
2. Click on **ATM**.	The Edit ATM Connector window opens.
3. Click on **Service Attributes**.	The ATM Service Records List window opens.
4. Click on **Add**.	The ATM Service Record Parameters window opens.
5. Click on **OK**.	The Select Protocols window opens.
6. Exit the Select Protocols window. You will add protocols later in "Adding IP, RIP or OSPF, and NHRP to the LEC Service Record" on page 2-17.	

Creating an MPOA Service Record

To run an MPOA server over ATM, you must first create an MPOA service record on an ATM interface. Then you add one or more MPOA servers to the MPOA service record.

To create an MPOA service record, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on an ATM link module interface (for example, **ATM1**).	The Select Connection Type window opens.
2. Click on **ATM**.	The Edit ATM Connector window opens.
3. Click on **MPOA Server Attributes**.	The MPOA Server Parameters window opens.
4. Click on **OK**.	The MPOA Service Record window opens.
5. Go to the next section, "Adding an MPOA Server (MPS)" on page 2-16, or go to the next step to exit this procedure.	
6. Click on **Done**.	You return to the Edit ATM Connector window.
7. Click on **Done**.	You return to the Select Connection Type window.
8. Click on **Done**.	You return to the Configuration Manager window.

By default, when you enter and then exit the MPOA Service Record window, you automatically create and enable the MPOA service record using the default settings. You need only enter and exit this window one time to create and enable the MPOA service record. However, for MPOA to operate, you must add at least one MPOA server (MPS) to the service record.

Note: You can have only one MPOA service record per ATM interface. However, this service record can contain up to four MPSs.

Adding an MPOA Server (MPS)

You must add at least one MPS to any MPOA service that you create on an ATM interface. Although not operational until fully configured, an MPS is enabled by default when you add it to an MPOA service record.

A new MPS must be in the enabled state so that you can map it to one or more LEC services. Then you have to map each MPS to a specific LEC service on the router.

To add an MPS to an MPOA service, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on an ATM link module interface (for example, **ATM1**).	The Select Connection Type window opens.
2. Click on **ATM**.	The Edit ATM Connector window opens.
3. Click on **MPOA Server Attributes**.	The MPOA Server Parameters window opens.
4. Click on **MPS**.	The MPS List window opens.
5. Click on **Add**.	The MPS Configuration Parameters window opens.
6. Click on **OK**.	You return to the MPS List window. The MPS List window shows the added MPS.
7. Repeat steps 5 and 6 to add additional MPOA servers.	
8. Click on **Done**.	You return to the MPOA Service Record window.
9. Click on **Done**.	You return to the Edit ATM Connector window.
10. Click on **Done**.	You return to the Select Connection Type window.
11. Click on **Done**.	You return to the Configuration Manager window.

Adding IP, RIP or OSPF, and NHRP to the LEC Service Record

To allow LANE and normally routed traffic to flow through an ATM LEC service and between MPSs, enable IP and optionally a routing protocol (RIP or OSPF) on that IP interface.

To allow NHRP address resolution requests and replies to flow through the same ATM LEC service and between MPSs, you must enable NHRP on that service.

To add protocols to an existing LEC service, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on the ATM interface (**ATM1**) on which you want to add protocols.	The Select Connection Type window opens.
2. Click on **ATM**.	The Edit ATM Connector window opens.
3. Click on **Service Attributes**.	The ATM Service Records List window opens.
4. Click on the ATM LANE service record to which you want to add protocols.	
5. Click on the Protocols menu in the upper left hand corner of the window.	
6. Choose **Add/Delete**.	The Select Protocols window opens.
7. Select **IP**, **RIP**, and **NHRP**.	
8. Click on **OK**.	The IP Configuration window opens.
9. Set the following parameters: • **IP Address** • **Subnet Mask** • **Transmit Bcast Addr** • **UnNumbered Assoc Addr** Click on **Help** or see *Configuring IP, ARP, RARP, RIP, and OSPF Services* for parameter descriptions.	
10. Click on **OK**.	The NHRP Network Configuration window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
11. Set the following parameters, or use default values: • **NHRP Request Path** *(View Only)* • **Client Enable** • **Client Reg Interval** • **Client Hold Time** • **Client Request Timeout** • **Client Request Retry** • **Client Max Pending Request Entries** • **Server Enable** • **Server Forward Enable** • **Server Max Next Hop Entries** • **Server Max Pending Request Entries** Click on **Help** or see *Configuring IP, ARP, RARP, RIP, and OSPF Services* for parameter descriptions.	
12. Click on **OK.**	You return to the ATM Service Records List window which displays a summary of the NHRP record that you configured.
13. Click on **Done**.	You return to the Edit ATM Connector window.
14. Click on **Done**.	You return to the Select Connection Type window.
15. Click on **Done**.	You return to the Configuration Manager window.

Mapping an MPS to the LEC Service Record

You must map an MPS to any LEC service likely to send and receive MPOA resolution requests and replies over the ATM network. You can map one MPS to one or more LEC services configured on the same ATM slot and connector.

To map an MPOA server (MPS) to a LEC service, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on an ATM link module interface (for example, **ATM1**).	The Select Connection Type window opens.
2. Click on **ATM**.	The Edit ATM Connector window opens.
3. Click on **MPOA Server Attributes**.	The MPOA Service Record window opens.
4. Click on **MPS**.	The MPS List window opens.
5. Click on **Mapping**.	The LEC (to) MPS Mapping List window opens.
6. Click on any LEC that you want to map to the MPS.	
7. Click on **Mapping**.	Site Manager maps the LEC to the MPS.
8. Repeat steps 8 and 9 to map any additional LECs.	
9. Click on **Done**.	You return to the MPS List window.
10. Click on **Done**.	You return to the MPOA Service Record window.
11. Click on **Done**.	You return to the Edit ATM Connector window.
12. Click on **Done**.	You return to the Select Connection Type window.
13. Click on **Done**.	You return to the Configuration Manager window.

Adding VRRP to the LEC Service Record

To configure a virtual router using Site Manager, complete the following tasks:

Caution: If you are configuring virtual routers on the IP interface used as the Site Manager management console, do not add or modify a backup virtual router before you create a master virtual router. Otherwise, you can lose connectivity to the router when dynamically configuring virtual routers. To prevent this, use local or remote mode when configuring a virtual router.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on **Add**.	The Add Virtual Router window opens.
5. Set the following parameters: • **Primary IP Address** • **Virtual Router ID** • **Virtual Router IP Address** Click on **Help** or see the parameter descriptions on page A-3.	
6. Click on **OK**.	You return to the IP VRRP Configuration Parameters window.

Chapter 3
Customizing VRRP

To customize VRRP, use the information in the following sections:

Topic	Page
Disabling and Reenabling a Virtual Router	3-2
Changing the IP Address Backed Up by a Virtual Router	3-3
Setting the Priority of the Virtual Router	3-4
Setting the Advertisement Interval	3-6
Setting the Critical IP Interface Address	3-8
Enabling or Disabling IPX Backup	3-9
Enabling or Disabling IGMP Backup	3-11
Setting the Token Ring Address	3-13

Caution: If you are configuring virtual routers on the IP interface used as the Site Manager management console, do not add or modify a backup virtual router before you create a master virtual router. Otherwise, you can lose connectivity to the router when dynamically configuring virtual routers. To prevent this, use local or remote mode when configuring a virtual router.

Disabling and Reenabling a Virtual Router

When you first configure a virtual router, the virtual router is enabled by default. You can use the BCC or Site Manager to disable or reenable a virtual router.

Using the BCC

To disable a virtual router, access the virtual router (for example, **box; ip; vrrp 192.41.31.21/2 vr-ip-address 192.41.31.22**) and enter:

state disabled

To enable a virtual router, access the virtual router and enter:

state enabled

For example, to disable a virtual router, enter the following command:

```
vrrp/192.41.31.21/2# state disabled
vrrp/192.41.31.21/2#
```

Using Site Manager

To disable or reenable a virtual router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on a virtual router instance ID to highlight it in the list of virtual routers.	The configuration that pertains to the highlighted virtual router appears.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-5.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Changing the IP Address Backed Up by a Virtual Router

When you first configure a virtual router, you must supply an IP address that the virtual router backs up. This IP address must be on the same subnet as the primary IP address. You can change the IP address to be backed up by a virtual router.

Using the BCC

To change the IP address to be backed up by a virtual router, access the virtual router (for example, **box; ip; vrrp 192.41.31.21/2 vr-ip-address 192.41.31.22**) and enter:

vr-ip-address <*vr_ip_address*>

For example, to change the IP address, enter the following command:

```
vrrp/192.41.31.21/2# vr-ip-address 192.41.31.25
vrrp/192.41.31.21/2#
```

Using Site Manager

To change the IP address to be backed up by a virtual router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on a virtual router instance ID to highlight it in the list of virtual routers.	The configuration that pertains to the highlighted virtual router appears.
5. Set the **Virtual Router IP Address** parameter. Click on **Help** or see the parameter description on page A-6.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Setting the Priority of the Virtual Router

You can set the priority of the virtual router in relation to all virtual routers that have the same virtual router ID and are on the same subnet. The higher you set the value, the higher the priority of the virtual router, and the more likely it will become primary if the master fails.

When you initially configure a virtual router, if the primary IP address is the same as the virtual router IP address, the priority is automatically set to the highest priority (255) and the virtual router becomes the master virtual router as soon as it comes up.

The default priority for all backup virtual routers is 100. You can set the priority for backup virtual routers from 1 to 254. If you assign more than one backup virtual router the same priority, the VRRP router with the greater primary IP address takes precedence.

Using the BCC

To change a virtual router's priority, access the virtual router (for example, **box; ip; vrrp 192.41.31.21/2 vr-ip-address 192.41.31.22**) and enter:

priority <*integer*>

integer is the priority from 1 to 255. (The priority values 0 and 255 are reserved for the master virtual router; the master uses priority 0 to indicate that it is releasing responsibility for the virtual router.)

For example, to change the priority to 254, enter the following command:

```
vrrp/192.41.31.21/2# priority 254
vrrp/192.41.31.21/2#
```

Using Site Manager

To set a virtual router's priority, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on a virtual router instance ID to highlight it in the list of virtual routers.	The configuration that pertains to the highlighted virtual router appears.
5. Set the **Priority** parameter. Click on **Help** or see the parameter description on page A-6.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Setting the Advertisement Interval

The advertisement interval is the number of seconds between transmissions of VRRP advertisements from the master virtual router notifying all backup routers that it is currently the master virtual router and is forwarding all traffic. You must set the same advertisement interval for all VRRP routers having the same VRID on the same LAN. The default advertisement interval is 1 second; however, you can change the interval to a value from 1 through 255.

Using the BCC

To change a virtual router's advertisement interval, access the virtual router (for example, **box; ip; vrrp 192.41.31.21/2 vr-ip-address 192.41.31.22**) and enter:

advertisement-interval <*integer*>

integer is the interval, in seconds, from 1 to 255.

For example, to change the advertisement interval to 60, enter the following command:

```
vrrp/192.41.31.21/2# advertisement-interval 60
vrrp/192.41.31.21/2#
```

Using Site Manager

To set the advertisement interval, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on a virtual router instance ID to highlight it in the list of virtual routers.	The configuration that pertains to the highlighted router appears.
5. Set the **Advertisement Interval** parameter. Click on **Help** or see the parameter description on page A-6.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Setting the Critical IP Interface Address

The critical IP interface resides on the same router as a physical interface. The state of the critical IP interface determines the state of the virtual router. If the critical interface fails, the virtual router fails and the VRRP router with the next highest priority becomes the master virtual router and begins routing traffic to its destination.

Using the BCC

To specify a critical IP interface address, access the virtual router (for example, **box; ip; vrrp 192.41.31.21/2 vr-ip-address 192.41.31.22**) and enter:

critical-ip-interface <*critical_ip_address*>

For example, to set the critical IP interface address, enter the following command:

```
vrrp/192.41.31.21/2# critical-ip-interface 192.41.31.76
vrrp/192.41.31.21/2#
```

Using Site Manager

To specify the critical IP interface address, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on a virtual router instance ID to highlight it in the list of virtual routers.	The configuration that pertains to the highlighted router appears.
5. Set the **Critical IP Interface** parameter. Click on **Help** or see the parameter description on page A-7.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Enabling or Disabling IPX Backup

When the Internetwork Packet Exchange (IPX) protocol is configured on the same physical interface as VRRP, you can enable IPX backup. When enabled, this feature provides IPX backup when the virtual router is in the master state. In this case, IPX configured on the physical interface uses the VRRP MAC address instead of the physical MAC address. If the virtual router is in the backup state, IPX is disabled.You can enable or disable IPX backup. By default, IPX backup is disabled.

You can enable IPX Backup for one virtual router per interface.

Using the BCC

To enable IPX backup, access the virtual router (for example, **box; ip; vrrp 192.41.31.21/2 vr-ip-address 192.41.31.22**) and enter:

ipx-backup enabled

To disable IPX backup, access the virtual router and enter:

ipx-backup disabled

For example, to enable IPX backup, enter the following command:

```
vrrp/192.41.31.21/2# ipx-backup enabled
vrrp/192.41.31.21/2#
```

Using Site Manager

To enable IPX backup, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on a virtual router instance ID to highlight it in the list of virtual routers.	The configuration that pertains to the highlighted router appears.
5. Set the **IPX Backup** parameter. Click on **Help** or see the parameter description on page A-7.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Enabling or Disabling IGMP Backup

When the Internet Group Management Protocol (IGMP) is configured on the same physical interface as VRRP, you can enable IGMP backup. When enabled, this feature provides IGMP backup when the virtual router is in the master state. In this case, IGMP configured on the physical interface is enabled. If the virtual router is in the backup state, IGMP is disabled. By default, IGMP backup is disabled.

You can enable IGMP Backup for one virtual router per interface.

Using the BCC

To enable IGMP backup, access the virtual router (for example, **box; ip; vrrp 192.41.31.21/2 vr-ip-address 192.41.31.22**) and enter:

igmp-backup enabled

To disable IGMP backup, access the virtual router and enter:

igmp-backup disabled

For example, to enable IGMP backup, enter the following command:

```
vrrp/192.41.31.21/2# igmp-backup enabled
vrrp/192.41.31.21/2#
```

Using Site Manager

To enable IGMP backup, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on a virtual router instance ID to highlight it in the list of virtual routers.	The configuration that pertains to the highlighted router appears.
5. Set the **IGMP Backup** parameter. Click on **Help** or see the parameter description on page A-8.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Setting the Token Ring Address

If you are running VRRP on a token ring network, VRRP uses the token ring functional address you provide instead of a virtual router MAC address. The token ring address setting identifies the token ring functional address for the virtual router MAC address that is configured on an IP interface over token ring.

However, if you are running VRRP on a token ring LANE network, packets with functional addresses are sent to the BUS and treated as multicast or broadcast frames, which causes the BUS to overload with user data frames. Since the BUS has limited packet throughput, you must supply a virtual router MAC address instead of a token ring functional address.

VRRP virtual MAC addresses have the following format:

00-00-5E-00-01-*XX*

where *XX* is the virtual router ID.

For instructions on supplying a token ring address, see “Configuring a Virtual Router” on page 2-2.

Caution: For virtual routers running over token ring, you must supply token ring functional addresses for virtual router MAC addresses, or VRRP will fail. However, for token ring LANE networks, you must supply virtual router MAC addresses.

Using the BCC

To set the token ring address, access the virtual router (for example, **box; ip; vrrp 192.41.31.21/2 vr-ip-address 192.41.31.22**) and enter:

token-ring-address <*address*>

address is one of the following unused token ring functional addresses:

- **03-00-02-00-00-00**
- **03-00-04-00-00-00**
- **03-00-08-00-00-00**
- **03-00-10-00-00-00**
- **03-00-20-00-00-00**
- **03-00-40-00-00-00**
- **03-00-80-00-00-00**
- **03-00-00-01-00-00**
- **03-00-00-02-00-00**
- **03-00-00-04-00-00**
- **03-00-00-08-00-00**

For example, to set the token ring address, enter the following command:

```
vrrp/192.41.31.21/2# token-ring-address 03-00-80-00-00-00
vrrp/192.41.31.21/2#
```

Using Site Manager

To set the token ring address, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on a virtual router instance ID to highlight it in the list of virtual routers.	The configuration that pertains to the highlighted router appears.
5. Set the **Token Ring Address** parameter. Click on **Help** or see the parameter description on page A-8.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Appendix A
Site Manager Parameters

This appendix contains the Site Manager parameter descriptions for VRRP services. You can display the same information using Site Manager online Help. For information about the IP parameters you must set so that you can configure VRRP, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*.

For each parameter, this appendix provides the following information:

- Parameter name
- Configuration Manager menu path
- Default setting
- Valid parameter options
- Parameter function
- Instructions for setting the parameter
- Management information base (MIB) object ID

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, see *Using Technician Interface Software*.

Caution: The Technician Interface does not verify the validity of your parameter values. Entering an invalid value can corrupt your configuration.

Add Virtual Router Parameters

The VRRP parameters in the Add Virtual Router window (Figure A-1) let you establish a virtual router on an IP interface.

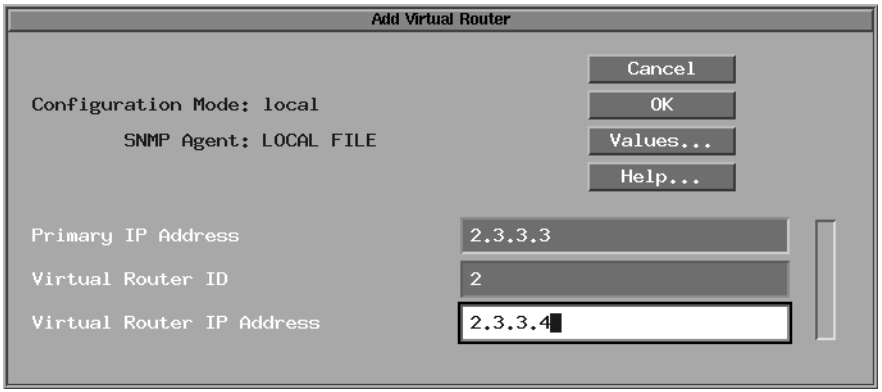

Figure A-1. Add Virtual Router Window

To access the Add Virtual Router window, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on **Add**.	The Add Virtual Router window opens.

The parameter descriptions follow.

Parameter: Primary IP Address

Path:	Configuration Manager > Protocols > IP > VRRP > Add
Default:	None
Options:	Any valid IP address in dotted-decimal notation
Function:	Identifies the IP address of the physical interface. The router lists this IP address as the source in VRRP advertisements sent by the virtual router.
Instructions:	Ensure that the primary IP address and the virtual router IP address are on the same subnet.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.25.1.1.4

Parameter: Virtual Router ID

Path:	Configuration Manager > Protocols > IP > VRRP > Add
Default:	None
Options:	1 to 255
Function:	Identifies the virtual router's ID (VRID). The router uses this number to calculate the MAC address. The VRID must be unique on the LAN segment.
Instructions:	Enter the ID of the virtual router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.25.1.1.5

Parameter: Virtual Router IP Address

Path:	Configuration Manager > Protocols > IP > VRRP > Add
Default:	None
Options:	Any valid IP address in dotted-decimal notation
Function:	Identifies the IP address that the virtual router backs up.
Instructions:	Ensure that the primary IP address and the virtual router IP address are on the same subnet. If the virtual router IP address is the same as the primary IP address, then this VRRP router, when operating, will always be the master virtual router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.25.1.1.6

VRRP Configuration Parameters

The VRRP configuration parameters let you customize a virtual router. You access these parameters from the IP VRRP Configuration Parameters window (Figure A-2).

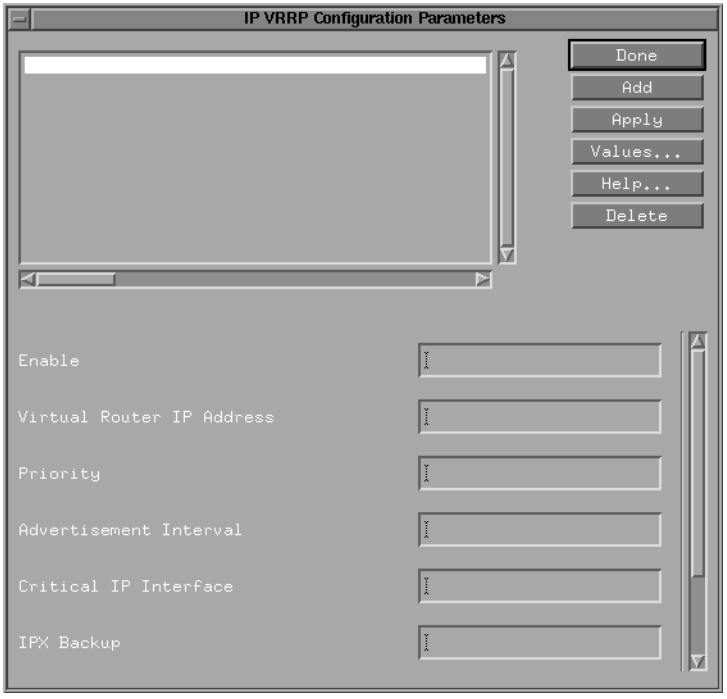

Figure A-2. IP VRRP Configuration Parameters Window

To access the IP VRRP Configuration Parameters window, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on a virtual router instance ID to highlight it in the list of virtual routers.	The configuration that pertains to the highlighted virtual router appears.

The parameter descriptions follow.

Parameter: Enable

Path: Configuration Manager > Protocols > IP > VRRP

Default: Enable

Options: Enable | Disable

Function: Enables or disables a virtual router on an interface.

Instructions: Select Enable to enable a virtual router on an interface. Select Disable to disable a virtual router on an interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.25.1.1.2

Parameter: Virtual Router IP Address

Path:	Configuration Manager > Protocols > IP > VRRP
Default:	None
Options:	Any valid IP address in dotted-decimal notation
Function:	Identifies the IP address of the interface that the virtual router backs up.
Instructions:	Enter the IP address that you want the virtual router to back up. Ensure that the primary IP address and the virtual router IP address are on the same subnet. If the virtual router IP address is the same as the primary IP address, Site Manager automatically sets the priority to 255 so that this VRRP router will always be the master virtual router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.25.1.1.6

Parameter: Priority

Path:	Configuration Manager > Protocols > IP > VRRP
Default:	100
Options:	1 to 255
Function:	Specifies the priority of the virtual router with respect to all virtual routers on the IP interface.
Instructions:	Enter a priority from 1 to 254. The higher the value you specify, the higher the priority of the virtual router. Site Manager automatically supplies a priority of 100 for all backup virtual routers. If you set the primary IP address to the IP address of the physical interface, Site Manager sets the priority to 255.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.25.1.1.8

Parameter: Advertisement Interval

Path:	Configuration Manager > Protocols > IP > VRRP
Default:	1 (s)
Options:	1 to 255
Function:	Specifies the interval, in seconds, between the transmission of VRRP advertisements from the primary virtual router.
Instructions:	Enter a value from 1 to 255 seconds.
MIB Object ID:	1.3.6.1.4.1.18.3.5.53.25.1.1.9

Parameter: Critical IP Interface

Path:	Configuration Manager > Protocols > IP > VRRP
Default:	0.0.0.0 (none)
Options:	Any valid IP address in dotted-decimal notation
Function:	Identifies an IP address that determines whether the virtual router assumes the role of the master virtual router and is responsible for forwarding traffic. If the critical IP address is operating, then the virtual router forwards traffic. If the critical IP address is down, then a backup virtual router assumes the responsibilities of the master virtual router and forwards traffic. The critical IP address must be on the same router as the primary IP address.
Instructions:	Specify an IP address on the same router where the primary IP address resides.
MIB Object ID:	1.3.6.1.4.1.18.3.5.53.25.1.1.10

Parameter: IPX Backup

Path:	Configuration Manager > Protocols > IP > VRRP
Default:	Disable
Options:	Enable | Disable
Function:	Enables or disables IPX backup when IPX is configured on the same physical interface as VRRP. When enabled, this feature provides IPX backup when the virtual router is in the master state. In this case, IPX configured on the physical interface uses the VRRP MAC address instead of the physical MAC address. If the virtual router is in the backup state, IPX is disabled.
Instructions:	Select Enable to enable IPX backup on the virtual router. Select Disable to disable IPX backup on the virtual router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.53.25.1.1.11

Parameter: IGMP Backup

Path: Configuration Manager > Select Protocols > IP > VRRP

Default: Disable

Options: Enable | Disable

Function: Enables or disables IGMP backup when IGMP is configured on the same physical interface as VRRP. When enabled, this feature provides IGMP backup when the virtual router is in the master state. In that case, IGMP configured on the physical interface is enabled. If the virtual router is in the backup state, IGMP is disabled.

Instructions: Select Enable to enable IGMP backup on the virtual router. Select Disable to disable IGMP backup on the virtual router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.53.25.1.1.12

Parameter: Token Ring Address

Path: Configuration Manager > Select Protocols > IP > VRRP

Default: None

Options: Use one of the following unused token ring functional addresses:

03-00-02-00-00-00
03-00-04-00-00-00
03-00-08-00-00-00
03-00-10-00-00-00
03-00-20-00-00-00
03-00-40-00-00-00
03-00-80-00-00-00
03-00-00-01-00-00
03-00-00-02-00-00
03-00-00-04-00-00
03-00-00-08-00-00

Function: Identifies the token ring functional address for the virtual router ID MAC address that is configured on an IP interface over token ring.

Instructions: Specify a unique functional token ring address. You must specify a token ring functional address for virtual routers on an IP interface over token ring; otherwise, VRRP will not function.

MIB Object ID: 1.3.6.1.4.1.18.3.5.53.25.1.1.13

Appendix B
Monitoring VRRP Using the BCC show Commands

This appendix describes how to use the BCC **show** command to obtain VRRP statistical data from the management information base (MIB). The type and amount of data displayed depend on the specific settings you want to view. This appendix includes descriptions of the following **show** commands:

Command	Page
show vrrp critical-ip-addresses	B-2
show vrrp mac-addresses	B-2
show vrrp summary	B-3

Online Help for show Commands

To display a list of command options, enter **show vrrp ?** at any BCC prompt. To learn more about any **show vrrp** command option and its syntax, use the question mark (**?**) command as follows:

Example

```
bcc> show vrrp?
critical-ip-addresses   mac-addresses            summary
bcc> show vrrp critical-ip-addresses?
show vrrp critical-ip-addresses [-vrid <arg>] [-primary-ip-address <arg>]
bcc>
```

show vrrp critical-ip-addresses

The **show vrrp critical-ip-addresses** command displays the local IP interface (critical IP address) associated with a specific VRRP virtual router or all VRRP virtual routers. This command allows for the following command filters (flags) and arguments:

-primary-ip-address <*primary_ip_address*>	Displays information about the virtual router associated with the IP address of the physical interface.
-vrid <*vrid*>	Displays information about the virtual router associated with the specified virtual router identifier.

The output includes the following information:

Primary IP Address	IP address of the physical interface with which the virtual router is associated.
VRID	Virtual router identifier configured in the range of 1 through 255.
Virtual IP Address	IP address that the virtual router backs up.
Critical IP Address	IP address that determines whether the virtual router assumes the role of the master virtual router and is responsible for forwarding traffic. If the critical IP address is operating, then the virtual router forwards traffic. If the critical IP address is down, then a backup virtual router assumes the responsibilities of the master virtual router and forwards traffic.

show vrrp mac-addresses

The **show vrrp mac-addresses** command displays the virtual media access control (MAC) address and token ring address associated with a specific VRRP virtual router or all VRRP virtual routers.

This command allows for the following command filters (flags) and arguments:

-primary-ip-address <*primary_ip_address*>	Displays information about the virtual router associated with the IP address of the physical interface.
-vrid <*vrid*>	Displays information about the virtual router that corresponds to the specified virtual router identifier.

The output includes the following information:

Primary IP Address	IP address of the physical interface with which the virtual router is associated.
VRID	Virtual router identifier configured in the range of 1 through 255.
Virtual IP Address	IP address that the virtual router backs up.
VRRP Virtual MAC Address	Virtual router MAC address that is configured on an IP interface over token ring
Token Ring Func. Address	Token ring functional address for the VRRP virtual MAC address.

show vrrp summary

The **show vrrp summary** command displays the state, advertisement interval, and priority for a specific VRRP virtual router or all VRRP virtual routers. This command allows for the following command filters (flags) and arguments:

-primary-ip-address <*primary_ip_address*>	Displays information about the virtual router associated with the IP address of the physical interface.
-vrid <*vrid*>	Displays information about the virtual router that corresponds to the specified virtual router identifier.

The output includes the following information:

Primary IP Address	IP address of the physical interface with which the virtual router is associated.
VRID	Virtual router identifier configured in the range of 1 through 255.
Virtual IP Address	IP address that the virtual router backs up.
VRRP Operational State	Current state of the virtual router: initialize, master, or backup.
Advertisement Interval	The interval, in seconds, between the transmission of VRRP advertisements from the primary virtual router.
Priority	The priority (from 1 through 255) of the virtual router with respect to all virtual routers on the IP interface.

Glossary

advertisement An IP packet periodically broadcast by the master virtual router to prevent a backup virtual router from becoming the master virtual router.

backup virtual router One of a set of VRRP routers available to become the master virtual router. A router may be either the master virtual router or the backup virtual router for many virtual routers.

critical IP interface A local IP interface associated with a virtual router. When the state of this interface changes, the virtual router switches roles. For example, if you designate IP address 1.1.1.1 as the critical IP address for virtual router 1 on router B, and IP address 1.1.1.1 fails, then virtual router 1 on router B is no longer the master virtual router, and a backup virtual router becomes the master virtual router.

master virtual router The VRRP router that both assumes responsibility for forwarding data packets received at the MAC address associated with its virtual router, and also answers ARP requests for its IP address. A router may be the master virtual router or the backup virtual router for many virtual routers.

primary IP address The real IP interface address used as the source IP address for the IP packets carrying advertisements.

priority The value that determines whether a virtual router serves as the master or backup virtual router. The VRRP router with the highest priority becomes the master virtual router. The value 255 is reserved for the router that owns the IP address associated with the virtual router. The value 0 is reserved for the master virtual router to indicate that it is releasing responsibility for the virtual router. The values 1 through 254 are available for VRRP routers backing up the virtual router. The default priority is 100.

virtual MAC address A unicast MAC address associated with each virtual router and used as the source MAC address for VRRP advertisements. The master virtual router uses this address instead of its physical MAC address in all communication.

virtual router	A software-defined object managed by VRRP that corresponds to an IP address on a LAN segment. A virtual router typically exists on multiple VRRP routers. One VRRP router acts as the master virtual router for this IP address, and the others act as backup virtual routers.
VRID	The virtual router identifier configured in the range of 1 through 255. The VRID must be unique within the subnet.
VRRP router	A physical router, not a virtual one, that runs the Virtual Router Redundancy Protocol. Typically, there are multiple VRRP routers in a network -- one master router and several backup routers.

Index

A

acronyms, xiii
adding
  ATM circuit, 2-13
  service records
    LANE, 2-14
adding a virtual router, 3-3
Advertisement Interval parameter, A-6
advertisement interval, setting, 3-6
ATM
  circuit, adding, 2-13
  starting with BCC, 2-7, 2-12

B

backup virtual router, defined, 1-2
BCC
  show commands, B-1
  starting ATM with, 2-7, 2-12
  starting VRRP services, 2-4, 2-11

C

configuring a multinetted interface, 2-2
configuring a virtual router, 2-1
conventions, text, xii
Critical IP Interface parameter, A-7
critical IP interface, specifying, 3-8
customer support, xiv

D

disabling
  a virtual router, 3-2
  IGMP backup, 3-11
  IPX backup, 3-9

E

Enable parameter, A-5
enabling
  a virtual router, 3-2
  IGMP backup, 3-11
  IPX backup, 3-9

I

IGMP Backup parameter, A-8
IGMP backup, enabling or disabling, 3-11
IP Address parameter
  IP configuration, 2-5
IP address to be backed up, assigning, 3-3
IP multicast datagrams, 1-2
IP, starting, 2-5
IPX Backup parameter, A-7
IPX backup, enabling or disabling, 3-9

L

LEC service records, 2-9

M

MAC address, 1-2, 2-2
master virtual router, defined, 1-2
messaging, 1-2
multinetted interface, configuring, 2-2

P

primary IP address, 2-2
Primary IP Address parameter, A-3
priority of virtual routers, defined, 1-2
Priority parameter, A-6
priority, setting, 3-4
product support, xiv
protocol messaging, defined, 1-2
publications, hard copy, xiv

R

redundancy services, planning, 1-3
router redundancy, characteristics, 1-3

S

service records
  adding
    LANE, 2-14
  defining
    LEC, 2-9
show commands, online Help for, B-1
show vrrp critical-ip-addresses command, B-2
show vrrp mac-addresses command, B-2
show vrrp summary command, B-3
signaling, enabling, 2-8
starting IP, 2-5
Subnet Mask parameter
  IP configuration, 2-5
support, Nortel Networks, xiv

T

technical publications, xiv
technical support, xiv
text conventions, xii
Token Ring Address parameter, A-8
token ring address, setting, 3-13
token ring functional address, 3-13
Transmit Bcast Addr parameter
  IP configuration, 2-5

U

UnNumbered Assoc Address parameter
  IP configuration, 2-5

V

virtual router
  configuring, 2-1
  disabling, 3-2
  enabling, 3-2
virtual router ID (VRID), assigning, 2-2
Virtual Router ID parameter, A-3
Virtual Router IP Address parameter, A-3, A-6
virtual router IP address, assigning, 2-2
VRRP advertisements, 3-6